Trellix
Manifesto for the new EU mandate (2024-29)

Introduction: Rising cyber security threats towards governments, international organisations and businesses

The quarterly reports from Trellix's advanced threat research centre's (ARC) elite team of security professionals and researchers indicate an intensification of attacks from nation-state actors, primarily Russia, China and North Korea.[1] These nations are engaged in digital espionage, disinformation campaigns, and cyberwarfare against Western governments, including EU institutions and Member States. APT groups and hacktivists are operating at their most prolific level since the war in Ukraine began two years ago. Major threat actors increasingly collaborate, motivated by political agendas and pragmatic goals, opting to share or sell their most valuable vulnerability discoveries on the open market, rather than hide them, leading to a proliferation of zero-day exploits. Trellix therefore welcomes the Council Strategic Agenda (2024-2029), which makes security and defence a key priority for the next five years.[2] It is right that the EU should step up its collective response to cyber and hybrid warfare, foreign manipulation and interference, as well as threats to critical infrastructure.

Amid escalating tensions in Europe, its neighbourhood and beyond, bolstering cyber security and defence capabilities stands as a strategic imperative for the EU – not only to fortify our own defence capabilities, but also to strengthen global and transatlantic security. Achieving success will require close collaboration with NATO and allied nations, coupled with leveraging private sector expertise and insights from international partners. Effective implementation of new cyber laws introduced in the last mandate will be pivotal in shaping Europe's cyber standards, which should draw on industry best practices while being internationally interoperable. Ensuring fair competition in vital digital markets like cyber security will not only reinforce European economic resilience and reduce strategic dependencies, but also create the conditions for a dynamic, secure, and trustworthy digital environment for citizens and companies alike.

Emerging technologies, such as generative AI and quantum computing, pose formidable threats to cyber security, necessitating policy adaptation, collaboration with the private sector, and further efforts to shorten the cyber skills gap. Trellix's collaboration at the European level, notably in dismantling the Genesis Market cybercriminal hub[3], showcases the efficacy of coordinated international efforts in concert between government and business. The Hungarian Presidency's priorities are pertinent in this regard by recognising that organised cybercrime is a threat to fundamental rights, critical infrastructure, and competitiveness.[4] The growing integration of digital processes in our daily lives expands

---

[1] https://www.trellix.com/advanced-research-center/threat-reports/june-2024/

[2] https://www.consilium.europa.eu/media/4aldqfl2/2024_557_new-strategic-agenda.pdf

[3] https://www.trellix.com/en-gb/blogs/research/genesis-market-no-longer-feeds-the-evil-cookie-monster/

[4] https://hungarian-presidency.consilium.europa.eu/media/32nhoe0p/programme-and-priorities-of-the-hungarian-presidency.pdf

the attack surface and amplifies the potential impact of cyber threats, posing escalating risks to people, businesses, and critical infrastructure. The stakes have never been higher to cybersecure our collective future.

Tackling cyber threats

The 2019-2024 EU mandate enacted important cyber security legislation to prevent, detect, and respond to cyber-attacks, including the recent Cyber Solidarity Act that establishes a reserve of trusted providers to assist EU institutions and national CSIRTs in responding to significant cyber incidents. While the Cyber Solidarity Act acknowledges the value of non-EU companies, the development of additional selection criteria in the procurement of trusted providers must ensure fair competition among providers from the EU and like-minded countries. This is essential for EU public authorities to access the most resilient, state-of-the-art solutions, while ensuring the robustness of the EU's cyber crisis preparedness and responsiveness.

To better detect and prevent cyber-attacks against critical infrastructure, we recommend that European policymakers develop the aggregate information sharing requirements of the Cyber Resilience Act (CRA) and the Network and Information Security Directive (NIS 2). The EU should develop bi-directional information sharing whereby governments aggregate private sector reporting, alongside the unique insights governments can generate, such that remediation of vulnerabilities is expedited and streamlined before threat actors can exploit them.

Recommendations:

- Develop selection criteria for cyber reserve procurement that ensures fair competition among providers from the EU and allied nations.
- Create mechanisms for bi-directional information sharing between business and government to detect and prevent cyber-attacks against critical infrastructure.

Ensuring global regulatory alignment

A key area where enhancing the international alignment of cyber security regulation is in the area of incident reporting and vulnerability reporting requirements. When definitions and timelines vary, it complicates the ability to compare cyber threat actors' behaviour, impact, and methods, and this is evident in the differing approaches in NIS2 and the CRA.

Given cyber security threats are inherently international, we recommend divergences in regulatory approaches to incident and vulnerability reporting are to be avoided. Hence, we encourage the incoming European Commission to deepen its information sharing agreement with US authorities, building on the December 2023 ENISA and US Cybersecurity and Infrastructure Security Agency (CISA) information sharing agreement on tackling growing security threats.

We also recommend that mutual recognition agreements are pursued in a range of policy areas, particularly focusing on certification, software bill of materials (SBOM), secure software development, and cloud security. Mutual recognition agreements in these areas

can ease burdens on organisations and may allow international organisations to operate within Europe and European countries to operate internationally with more ease.

Recommendations:

- Enhance information sharing agreements with US counterparts.
- Promote mutual recognition agreements on certification, software bill of materials (SBOM), secure software development and cloud security.

Promoting a fair and competitive cyber security environment to improve resilience

Restrictive software licensing limits customer choice, raises costs for customers and increases cyber vulnerabilities. Purposefully opaque and complex software licenses create artificial barriers to switching and lock customers into their ecosystem.

Such restrictive software licensing is a threat to competition as more and more of the cloud ecosystem are controlled by a few legacy software providers. This threat to competition extends beyond the cloud as restrictive software licensing can grow dominance in other markets including cyber security and video collaboration. In nascent markets like AI, this behaviour has the ability to shift the future of the industry, especially where shortages of supply in advanced semiconductors and skilled engineers creates bottlenecks in developing state-of-the-art AI models.

Restrictive licensing isn't just a competition problem - it's a cyber security problem that can harm national security. Restrictive licensing builds a technology monoculture that spreads the same software and hardware across entire companies and even governments.

Indeed, there are inherent dangers in relying on single vendor ecosystems in the cyber security context. Strong defence requires implementation of best-of-breed technologies, in which no single vendor has a silver bullet. We recommend European policymakers and competition authorities pursue policies that encourage vendor diversification in our cyber security solutions such that public and private organisations have the opportunity to choose true best-of-breed solutions and expertise.

Recommendations:

- Ensure the DMA remains future-proof and fit for purpose in fast-evolving digital markets, including by:
    - addressing market realities where gatekeepers tie critical digital services, like cyber security software, to their core platforms, which limits contestability.[5]
    - ensuring that business users may also be counted as end users when using cloud services, which should cover IaaS, as well as PaaS and SaaS.
    - ensuring that third party software is fully interoperable with large cloud providers' services, designated as core platform services as appropriate to avoid tying practices and enable user switching.

[5] In accordance with Article 12 of the DMA.

- monitoring investments, partnerships and recruitment strategies that provide unfair advantages to cloud providers in adjacent markets, such as the provision of foundation models and generative AI applications, which can also be integrated into productivity software, providing network effects and discouraging adoption of alternative solutions. This may also consider whether Model-as-a-Service (MaaS) merits inclusion in the list of core platform services, as they become central to gatekeepers' business models.

Building a strong Cyber Defence environment

The war in Ukraine shows the strategic relevance of building a strong cyber defence environment. When cyber and hybrid attacks surged in Ukraine, various global and European stakeholders played a crucial role. Trellix, already present in the country before the war started, worked in concert with international partners to address the surge of cyber-attacks.

Cyber-attacks do not target only government and military entities; they reach critical infrastructure, public services, and the media sector amongst other sectors, all impacting governments' ability to run a country, lead an army, ensure business continuity and citizens' access to information and essential services.

Strengthening EU defence capabilities is rightly a priority under the next EU mandate. Still, this cannot happen without addressing cyber security risks and reinforcing the cyber resilience of critical infrastructures. Mechanisms set up by the Cyber Solidarity Act constitute a good basis, particularly the EU Cybersecurity Reserve. However, it is essential that the financial resources allocated to this instrument are commensurate with the risks European businesses and citizens face in this changed environment.

In addition, the promotion of public-private partnerships within the European Cyber Shield - along with the development of national and cross-border SOCs - is the right approach to bolster the EU's cyber defence and foster an environment conducive to mutual learning and growth. Drawing from our extensive experience of more than 15 years with similar collaborations, such as with the DHS, NIST, NSTAC, IT-SCC, JCDC, and NCCoE , we can attest to the value these partnerships offer.

Recommendations:

- Encourage public-private partnerships on threat intelligence with the participation of experienced companies with global connections from like-minded countries in the "Trusted Partners" category.
- Set up rapid intervention mechanisms, using to this end the Cyber Reserve created under the Cyber Solidarity Act and/or additional levers.
- Involve private industry and NIS2 entities in the mapping of cyber security capacity and work-streams under the Cyber Solidarity Act.

Implement legislation aimed at reinforcing businesses' and public administration's cyber security

The 2019-2024 EU mandate has seen the adoption of a range of new regulations in the cyber security space. The co-legislators adopted a number of laws to reinforce businesses' and public administration's cyber security, amongst which the NIS2 Directive increases the number of entities (from 15 000 covered by the NIS1 Directive to more than 110 000) falling into its scope and harmonises stronger cyber security rules across Member States.

The EUIBAs Regulation creates new cyber security requirements for all EU institutions, bodies and agencies (EUIBAs), whilst the Cyber Resilience Act increases security across the digital supply chain by promoting and mandating global cyber security practices.

Now is time to make sure these pieces of legislation are properly implemented: the NIS2 Directive has to be transposed by Member States by October 2024, the EUIBAs Regulation is set to operate at full scale in 2024-2025 and has the potential to inspire other public administrations across the EU, and harmonized standards should be developed for the cyber security and vulnerability handling requirements stemming from the Cyber Resilience Act before these requirements apply in 2027.

In particular, mutual recognition agreements or the use of international standards is critical to ensure a level playing field. Hence, we strongly support the ongoing work on a mutual recognition agreement between the Cyber Resilience Act in the EU and the Cyber Trust Mark in the US to ensure that manufacturers can focus on their products and not the steps necessary for individual validation processes.

Recommendations:

- Make sure Member States transpose and implement the NIS2 Directive in due time.
- Implement the EUIBAs Regulation and promote it as a best practice across Member States.
- When creating standards, in particular the framework of the Cyber Resilience Act, take into account existing international standards that can ensure compliance and involve the industry in the development of new standards.

Future challenges

The regulations adopted during the 2019-2024 mandate have tackled – rightfully – the cyber security of critical infrastructures, including in the financial sector, of products and of the EU institutions. Still, and while the EU has set the objective of more than 90% of SMEs reach at least a basic level of digital intensity by 2030, SMEs overall remain poorly protected against cyber-attacks and need to improve their resilience to cyber-attacks and achieve at least basic levels of cyber security. The next EU mandate could provide financial and non-financial incentives to this end, such as requirements to show adequate level of cyber security in public procurements, the establishment of a voucher scheme for SMEs, and the recognition of the US Cyber Trust Mark or the establishment of a similar mechanism at EU level.

By harnessing generative AI, organisations can identify emerging threats with unprecedented speed and accuracy, thereby strengthening their defences against cyber-attacks. Yet, AI can also be exploited by cyber criminals without technical knowledge to outstrip traditional defence mechanisms. This includes the development of new forms of malware that eludes detection and disrupts remediation, or sophisticated social engineering and phishing attacks that scale faster and tailor specifically to targets. Quantum computing similarly poses a significant threat to cyber security since it could break current forms of encryption. Understanding this increasingly complex landscape, and possibly adapting policies accordingly, will be a key challenge under the next EU mandate, requiring expertise from the private sector.

Beyond the evolving technological landscape, it is clear that the private sector plays a pivotal role in delivering cyber security intelligence, products and services, exemplified by Trellix's extended detection and response (XDR) platform. Leveraging their expertise in the state of the art of cyber security, private stakeholders from the EU and allied nations should be equally engaged in forthcoming cyber security initiatives, precisely because of escalating geopolitical tensions.

Trellix supports the Commission's efforts to bridge the cyber security skills gap. This scarcity undermines European defence and security, which is being targeted by nation-state actors. Europe should invest in current talent, while actively recruiting from underrepresented groups and other fields with transferable skills. We've embraced a flexible approach to professional development, revising our job descriptions to prioritise skills, which can be nurtured, over academic degrees and industry experience. By removing barriers to entry, we enhanced recruitment agility and diversified our workforce. Given the shortage of STEM graduates in Europe, ENISA's European Cybersecurity Skills Framework (ECSF) could consider accommodating more dynamic skills sets beyond traditional IT domains, such as gamers and ex-military.

In the US, the movement of cyber professionals between sectors enhances cyber readiness. EU policymakers should promote such cross-pollination to leverage diverse cyber security experiences gained in industry and government. The US Department of Defense Cyber Scholarship Program not only commits individuals to government service but also provides comprehensive training, preparing them for private sector roles if they choose to transition. The Commission should explore launching similar capacity-building initiatives in the EU.

Recommendations:

- Set an EU cyber security target for SMEs.
- Establish a *Cyber4EU* voucher scheme for SMEs.
- Involve the private sector in the forums and mechanisms aimed at understanding the evolving cyber threat landscape and the use of technology, as well as in any cyber security related upcoming initiatives.
- Consider incentives to encourage organisations operating in the EU to broaden their cyber job profiles and candidate expectations.
- Explore initiatives that not only make cyber security roles more accessible within public authorities but also provide rigorous training for skills that can also be deployed in different contexts.

About Trellix

Trellix is a global company redefining the future of cyber security. Our open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix was formed in 2021 by the combination of McAfee Enterprise and FireEye Products. This combination created a cyber security market leader with more than 40,000 customers, 5,000 employees, over $2Bn of annual revenue and serve more than 80% of the Fortune 100 companies.

As an enterprise and government security vendor, we are dedicated to transforming the way organizations think about digital security by delivering best-in-class technology and expertise. Today's dynamic threat landscape requires a holistic, integrated ecosystem and a cloud-first approach allowing all security products to work in unison.

Our integrated security portfolio protects customers across endpoints, infrastructure, applications, and in the cloud. Our open and native extended detection and response (XDR) platform provides a holistic ecosystem that consolidates security products into an interconnected, constantly communicating platform that's always learning and adapting to new and evolving threats.

By harnessing the power of machine learning and automation to unlock insights and streamline workflows, Trellix helps organizations stay one step ahead of adversaries, adapt to new threats, and accelerate detection and correction through the entire cyber defence lifecycle.

https://www.trellix.com/en-us/index.html

https://www.trellix.com/about/public-policy/

For further information please contact:
Chris Hutchins
Managing Director Public Policy
Chris.Hutchins@trellix.com

EU Transparency Register n°848399332282-85